

0418017-5NY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212454

(43)Date of publication of application : 06.08.1999

(51)Int.Cl.

G09C 1/00

G11B 20/10

(21)Application number : 10-015666

(71)Applicant : MATSUMOTO TSUTOMU
NHK SPRING CO LTD

(22)Date of filing : 28.01.1998

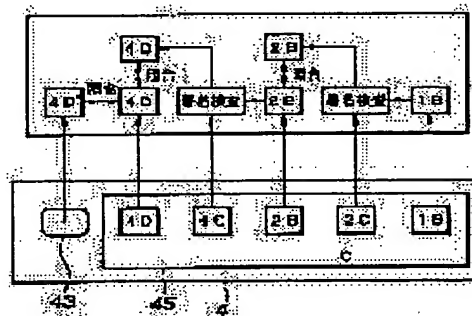
(72)Inventor : MATSUMOTO TSUTOMU
MATSUMOTO HIROYUKI
YAMAMOTOYA KENJI

(54) AUTHENTICATION TYPE SECURITY SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To effectively prevent an authenticated body from being forged, to facilitate the maintenance, and to evade complexity of the structure of, specially, the authenticated body side by collating feature data with physical features which are read at the time of authentication and deciding whether or not the authenticated body is genuine or false according to the respective matching results.

SOLUTION: When a card 4 to be authenticated is inserted into a card reader 3, issue device sign data 4c, feature data 4C, etc., stored on a magnetic stripe 45 are read out and physical features are read as feature data 4D' out of a reference area 43 along a read track set on the card reader 3. The authentication device sign data 2C are deciphered with authentication device open key data 1B and collated with issue device open key data 2B. Issue device sign data 4C are deciphered with the issue device open key data 2B and collated with feature data 4D. The feature data 4D' and feature data 4D are collated with each other. When the respective collated results meet specific conditions, it is decided that the card 4 is a regular card.



LEGAL STATUS

[Date of request for examination]

07.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-212454

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.⁸

G 0 9 C 1/00

識別記号

6 4 0

F I

G 0 9 C 1/00

6 4 0 B

6 4 0 D

G 1 1 B 20/10

G 1 1 B 20/10

H

審査請求 未請求 請求項の数 8 O L (全 10 頁)

(21) 出願番号 特願平10-15666

(22) 出願日 平成10年(1998) 1月28日

(71) 出願人 596048536

松本 勉

神奈川県横浜市青葉区柿の木台13番地45

(71) 出願人 000004640

日本発条株式会社

神奈川県横浜市金沢区福浦3丁目10番地

(72) 発明者 松本 勉

神奈川県相模原市上鶴間2603-1 サンヴ

ェール町田グランデュール210

(72) 発明者 松本 弘之

神奈川県横浜市金沢区福浦3丁目10番地

日本発条株式会社内

(74) 代理人 弁理士 大島 陽一

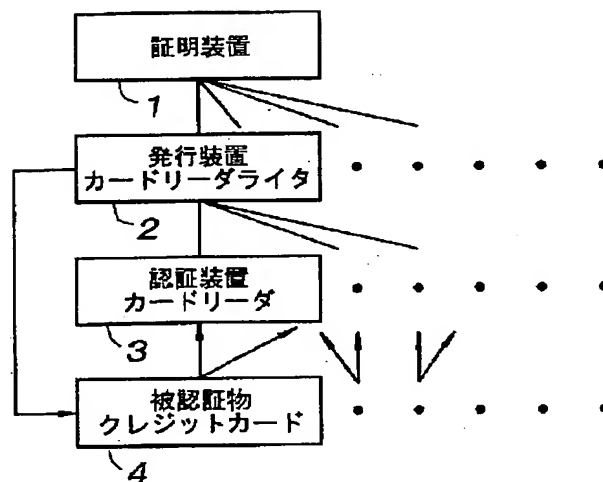
最終頁に続く

(54) 【発明の名称】 認証式セキュリティシステム

(57) 【要約】

【課題】 被認証物の偽造を防止し得ると共に保守が容易であり、特に被認証物側の構造も複雑化することのないセキュリティシステムを提供する。

【解決手段】 基準領域の物理的特徴データ、この特徴データを発行装置用秘密鍵データにより暗号化した署名データ及び発行装置用公開鍵データを被認証物のデータ格納領域に格納し、これを認証時に読み出すと共にその基準領域の特徴を読み取り、これらの照合結果により被認証物の真正性を確認可能としたため、秘密鍵データを知らずに署名データを解析することは困難であり、また被認証物に格納されたデータを単にデッドコピーしても他の被認証物では基準領域の特徴が異なることからその真正性は否定されるため他の被認証物への不正な適用をも防止でき、しかも認証に必要なデータが全て被認証物側にあることから、認証装置側の記憶容量を著しく低減でき、また秘密鍵・公開鍵データの変更、追加しても認証装置側の更新を必要とせずその保守が簡便になる。



【特許請求の範囲】

【請求項 1】 証明装置が証明した発行装置が発行した被認証物を認証装置をもって認証することでその真正性の判定を行い、前記被認証物の偽造を防止するためのセキュリティシステムであって、

前記被認証物が、機械により読み取り可能であるが、無作為に生成されているために人為的に同一なものを製作することが困難な物理的特徴を有する基準領域と、発行時に前記基準領域から読み取った特徴データ、該特徴データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる発行装置署名データ及び前記発行装置署名データを復号するための発行装置用公開鍵データを記憶保持するためのデータ格納領域とを有し、

認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された特徴データ、発行者署名データ及び発行装置用公開鍵データを読み出すと共に前記基準領域からその物理的特徴を読み取り、

前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、

前記特徴データと、認証時に読み取った物理的特徴とを照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする認証式セキュリティシステム。

【請求項 2】 前記被認証物が、連続するまたは不連続な複数の基準領域を有し、かつ前記データ格納領域が、前記各基準領域に対応する特徴データ及びそれに対応する発行装置署名データを記憶保持するようになっており、

認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された発行装置用公開鍵データを読み出すと共に選択的に 1 つまたは複数の特徴データ及びそれに対応する発行装置署名データを読み出し、更に前記読み出した特徴データに対応する基準領域からその物理的特徴を読み取り、

前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、

前記特徴データと、認証時に読み取った物理的特徴とを照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項 1 に記載の認証式セキュリティシステム。

【請求項 3】 前記被認証物が、演算処理部を更に有し、かつ前記データ格納領域が、被認証物毎に設定される被認証物用秘密鍵データ、被認証物用公開鍵データ及び前記被認証物用公開鍵データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる別の発行装置署名データを更に記憶保持するようになっており、

認証時に、前記データ格納領域から被認証物用公開鍵データ及び前記別の発行装置署名データをも更に読み出

し、

前記発行装置用公開鍵データをもって前記被認証物署名データを復号して前記被認証物用公開鍵データと照合し、

前記認証装置から認証の度に異なる確認データを前記被認証物に送り、その前記演算処理部にて前記被認証物用秘密鍵データにより前記確認データを暗号化して前記認証装置に送り返し、該認証装置にて前記被認証物用公開鍵データをもって復号して前記確認データと照合し、前記特徴データと、認証時に読み取った物理的特徴とを照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項 1 または請求項 2 のいずれかに記載の認証式セキュリティシステム。

【請求項 4】 前記確認データが認証時に読み取った物理的特徴に基づき生成されるようになっていることを特徴とする請求項 3 に記載の認証式セキュリティシステム。

【請求項 5】 前記被認証物の前記データ格納領域が、前記発行装置用公開鍵データを前記証明装置にて証明装置用秘密鍵データにより暗号化してなる証明装置署名データ及び前記証明装置用秘密鍵データにより暗号化された証明装置署名データを復号するための証明装置用公開鍵データをも更に格納するようになっており、

認証時に前記証明装置署名データ及び前記証明装置用公開鍵データをも読み出し、

前記証明装置用公開鍵データをもって前記証明装置署名データを復号したものと前記発行装置用公開鍵データとを更に照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項 1乃至請求項 4 のいずれかに記載の認証式セキュリティシステム。

【請求項 6】 前記認証装置が前記証明装置と接続可能となっており、かつ過去の認証時に被認証物から読み出された証明装置用公開鍵データを 1 つまたは 2 つ以上記憶可能となっており、

認証時に被認証物から読み出された証明装置用公開鍵データを記憶された証明装置用公開鍵データと比較し、一致すれば該証明装置用公開鍵データを用いて前記照合を行い、一致しなければ前記証明装置に問い合わせた正規の証明装置用公開鍵データであることが確認されたら該証明装置用公開鍵データを用いて前記照合を行うと共にこれを記憶するようになっていることを特徴とする請求項 5 に記載の認証式セキュリティシステム。

【請求項 7】 前記被認証物の前記データ格納領域が、前記発行装置用公開鍵データを前記証明装置にて証明装置用秘密鍵データにより暗号化してなる証明装置署名データをも更に格納するようになっており、

前記認証装置が、前記証明装置用秘密鍵データにより暗号化された証明装置署名データを復号するための証明装置用公開鍵データを記憶しており、

認証時に前記証明装置署名データをも読み出し、前記証明装置用公開鍵データをもって前記証明装置署名データを復号したものと前記発行装置用公開鍵データとを更に照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていないことを特徴とする請求項 1 乃至請求項 4 のいずれかに記載の認証式セキュリティシステム。

【請求項 8】 前記基準領域が、紙または樹脂中に磁性体繊維を無作為に配置したものからなることを特徴とする請求項 1 乃至請求項 7 のいずれかに記載の認証式セキュリティシステム。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】本発明は、例えばプリペイドカード、クレジットカード、ＩＤカードなどの真正性の判定を要する被認証物の偽造を防止するためのセキュリティシステムに関する。

【0002】

【従来の技術】従来のセキュリティシステムの 1 つの手法として、証明装置（機関）と、発行装置（機関）とにより、秘密鍵データによる署名生成ルールを用いて元のデータから署名データを生成し、これをクレジットカード等の被認証物に例えば磁気記録し、該被認証物を発行し、認証装置に記憶された公開鍵データから署名検査ルールを用いて上記署名データを検査してこの被認証物を認証することによりその真正性を確認する認証システムが知られている。

【0003】このシステムによれば、署名生成ルールを知る者のみが、自らの署名データを新たに生成したり、当該データを改変することができることから、新たな被認証物を装う偽造行為に対する防止効果は高いものの、例えば認証装置と被認証物との間の通信を傍受したり被認証物から署名データを読み出してデッドコピーすることによる不正は防止できない。

【0004】一方、被認証物の偽造や複製を防止する手段として、例えばその被認証物に固有の物理的な特徴をデータとして記録し、このデータと実際の物理的な特徴とを照合して真正性を判定する方法も提案されている。

【0005】そこで、本願出願人は、例えば特願平 8-85946 号明細書に記載されているように、各被認証物毎の物理的な特徴データを上記署名データとしてその被認証物に記録し、認証時に被認証物の物理的特徴を読み取ると共にこの署名データを特徴データに戻して両者を比較する方法を提案した。

【0006】この方法によれば、被認証物の記録内容を知ってもその被認証物毎の物理的な特徴をも模倣しない

限り偽造することはできないことからその偽造防止効果は著しく高くなる。

【0007】

【発明が解決しようとする課題】しかしながら、上記証明装置と、発行装置とが同一であり、かつこれらと認証装置とが一対一対応であれば良いが、例えばクレジットカードの場合、通常、証明装置（クレジット会社）と、発行装置（クレジット会社、銀行等）とは同一の機関である可能性はあるもののこれらとクレジットカードを使用する店などに設置される認証装置とは別々の機関であることが多く、特に発行装置に比較して認証装置が著しく多い。従って、上記秘密鍵データや公開鍵データを変更する場合や発行装置（機関）が増減する場合、その度に各認証装置に記憶された公開鍵データ等を変更しなければならず、その保守が厄介であった。

【0008】一方、被認証物側に IC による演算処理部を設け、認証の度に認証装置から被認証物に乱数等の確認データを秘密鍵データにより生成した署名データを送り、これを公開鍵データにより元の確認データに戻して送り返す動作を付加し、認証装置と被認証物側との間の通信内容を認証の度に変える動的認証方法も提案されているが、被認証物側で複雑な計算を行わなければならないことから、そのための IC が大型化、高騰化する問題があった。

【0009】このような従来技術の問題に鑑み、本発明の主な目的は、被認証物の偽造を効果的に防止し得ると共に保守が容易であり、特に被認証物側の構造も複雑化することのないセキュリティシステムを提供することにある。

【0010】

【課題を解決するための手段】上記の目的は本発明によれば、発行装置が発行し、かつ証明装置が証明した被認証物を認証装置をもって認証することでその真正性の判定を行い、前記被認証物の偽造を防止するためのセキュリティシステムであって、前記被認証物が、機械により読み取り可能であるが、無作為に生成されているために人為的に同一なものを製作することが困難な物理的特徴を有する基準領域と、発行時に前記基準領域から読み取った特徴データ、該特徴データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる発行装置署名データ及び前記発行装置用秘密鍵データにより暗号化された発行装置署名データを復号するための発行装置用公開鍵データを記憶保持するためのデータ格納領域とを有し、認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された特徴データ、発行装置署名データ及び発行装置用公開鍵データを読み出すと共に前記基準領域からその物理的特徴を読み取り、前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、前記特徴データと、認証時に読み取った物理的特徴とを照合し、前記各照合結果に基

づき前記被認証物の真正性の判定が行われるようになって、しかも処理が簡便になる。

【0013】基準領域として、紙又は樹脂中に磁性体繊維を無作為に配置したものや、紙の漉きむらを利用したり、シート材の表面粗さなど、人為的に複製することが困難で、しかも所定の機械では再現性良く検出し得るものであれば、任意のものをを用いることができる。そのような例としては、特開平 6-168363 号、特開昭 52-33444 号、特表昭 57-500851 号の各公報に開示されたものなどがある。

【0014】

【発明の実施の形態】以下、本発明の好適実施形態を添付の図面について詳しく説明する。

【0015】図 1 は、本発明が適用された第 1 の実施形態における認証式セキュリティシステムの概略構成を示すブロック図である。このシステムは、クレジットカードにおける認証式セキュリティシステムであり、証明装置 1 が 1 つまたは複数設置された証明機関（カード会社）と、カードの発行装置としてのカードリーダライタ 2 が 1 つまたは複数設置された発行機関（銀行、代理店等）と、認証装置としてのカードリーダ 3 が 1 つまたは複数設置された認証者（カードを使用する店、施設等）と、通常は多数発行される被認証物としてのクレジットカード 4 とから構成される。

【0016】図 2 は、クレジットカード 4 を示す平面図であり、このクレジットカード 4 はポリエステル製のベースシート 41 からなり、このカードには、発行者、券種やカードの用途を特定するために必要な管理データとは別に、後記する特徴データ、発行装置署名データ、発行装置用公開鍵データ、証明装置署名データ及び証明装置用公開鍵データを格納するための識別データ格納領域を含む磁気ストライプ 42 と、磁性体繊維をベースシート 41 の樹脂中に無作為に分散してなる基準領域 43 とが設けられている。

【0017】図 3 は、本発明が適用された発行装置としてのカードリーダライタ 2 を示す。カードリーダライタ 2 は、カードをスロット 21 内に取り込み、データ書き込み後にカードを排出するためのモータ駆動されたローラを含むカード搬送ユニット 22 が内蔵されている。スロット 21 に沿って、磁気ストライプ 42 から磁気データを読み出し／書き込みするための磁気ヘッド 23 及び基準領域 43 を読み取るための誘導式磁気ヘッド 24 が設けられている。磁気ヘッド 23、24 はその入出力を制御すると共にデータ処理を行うための制御ユニット 25 に接続されている。尚、実際に発行されたカードを認証するための認証装置としてのカードリーダ 3 は書き込み機能を除き、カードリーダライタ 2 と同様であるのでその詳細な説明を省略する。

【0018】以下に、図 4～図 6 に沿ってカード 4 の発行手順及び認証手順を説明する。証明装置 1 は、証明装置用秘密鍵データ 1A を用いて特定の署名生成ルールに

づき前記被認証物の真正性の判定が行われるようになって、しかも処理が簡便になる。

【0013】基準領域として、紙又は樹脂中に磁性体繊維を無作為に配置したものや、紙の漉きむらを利用したり、シート材の表面粗さなど、人為的に複製することが困難で、しかも所定の機械では再現性良く検出し得るものであれば、任意のものをを用いることができる。そのような例としては、特開平 6-168363 号、特開昭 52-33444 号、特表昭 57-500851 号の各公報に開示されたものなどがある。

【0014】

【発明の実施の形態】以下、本発明の好適実施形態を添付の図面について詳しく説明する。

【0015】図 1 は、本発明が適用された第 1 の実施形態における認証式セキュリティシステムの概略構成を示すブロック図である。このシステムは、クレジットカードにおける認証式セキュリティシステムであり、証明装置 1 が 1 つまたは複数設置された証明機関（カード会社）と、カードの発行装置としてのカードリーダライタ 2 が 1 つまたは複数設置された発行機関（銀行、代理店等）と、認証装置としてのカードリーダ 3 が 1 つまたは複数設置された認証者（カードを使用する店、施設等）と、通常は多数発行される被認証物としてのクレジットカード 4 とから構成される。

【0016】図 2 は、クレジットカード 4 を示す平面図であり、このクレジットカード 4 はポリエステル製のベースシート 41 からなり、このカードには、発行者、券種やカードの用途を特定するために必要な管理データとは別に、後記する特徴データ、発行装置署名データ、発行装置用公開鍵データ、証明装置署名データ及び証明装置用公開鍵データを格納するための識別データ格納領域を含む磁気ストライプ 42 と、磁性体繊維をベースシート 41 の樹脂中に無作為に分散してなる基準領域 43 とが設けられている。

【0017】図 3 は、本発明が適用された発行装置としてのカードリーダライタ 2 を示す。カードリーダライタ 2 は、カードをスロット 21 内に取り込み、データ書き込み後にカードを排出するためのモータ駆動されたローラを含むカード搬送ユニット 22 が内蔵されている。スロット 21 に沿って、磁気ストライプ 42 から磁気データを読み出し／書き込みするための磁気ヘッド 23 及び基準領域 43 を読み取るための誘導式磁気ヘッド 24 が設けられている。磁気ヘッド 23、24 はその入出力を制御すると共にデータ処理を行うための制御ユニット 25 に接続されている。尚、実際に発行されたカードを認証するための認証装置としてのカードリーダ 3 は書き込み機能を除き、カードリーダライタ 2 と同様であるのでその詳細な説明を省略する。

【0018】以下に、図 4～図 6 に沿ってカード 4 の発行手順及び認証手順を説明する。証明装置 1 は、証明装置用秘密鍵データ 1A を用いて特定の署名生成ルールに

づき前記被認証物の真正性の判定が行われるようになって、しかも処理が簡便になる。

【0013】基準領域として、紙又は樹脂中に磁性体繊維を無作為に配置したものや、紙の漉きむらを利用したり、シート材の表面粗さなど、人為的に複製することが困難で、しかも所定の機械では再現性良く検出し得るものであれば、任意のものをを用いることができる。そのような例としては、特開平 6-168363 号、特開昭 52-33444 号、特表昭 57-500851 号の各公報に開示されたものなどがある。

【0014】

【発明の実施の形態】以下、本発明の好適実施形態を添付の図面について詳しく説明する。

【0015】図 1 は、本発明が適用された第 1 の実施形態における認証式セキュリティシステムの概略構成を示すブロック図である。このシステムは、クレジットカードにおける認証式セキュリティシステムであり、証明装置 1 が 1 つまたは複数設置された証明機関（カード会社）と、カードの発行装置としてのカードリーダライタ 2 が 1 つまたは複数設置された発行機関（銀行、代理店等）と、認証装置としてのカードリーダ 3 が 1 つまたは複数設置された認証者（カードを使用する店、施設等）と、通常は多数発行される被認証物としてのクレジットカード 4 とから構成される。

【0016】図 2 は、クレジットカード 4 を示す平面図であり、このクレジットカード 4 はポリエステル製のベースシート 41 からなり、このカードには、発行者、券種やカードの用途を特定するために必要な管理データとは別に、後記する特徴データ、発行装置署名データ、発行装置用公開鍵データ、証明装置署名データ及び証明装置用公開鍵データを格納するための識別データ格納領域を含む磁気ストライプ 42 と、磁性体繊維をベースシート 41 の樹脂中に無作為に分散してなる基準領域 43 とが設けられている。

【0017】図 3 は、本発明が適用された発行装置としてのカードリーダライタ 2 を示す。カードリーダライタ 2 は、カードをスロット 21 内に取り込み、データ書き込み後にカードを排出するためのモータ駆動されたローラを含むカード搬送ユニット 22 が内蔵されている。スロット 21 に沿って、磁気ストライプ 42 から磁気データを読み出し／書き込みするための磁気ヘッド 23 及び基準領域 43 を読み取るための誘導式磁気ヘッド 24 が設けられている。磁気ヘッド 23、24 はその入出力を制御すると共にデータ処理を行うための制御ユニット 25 に接続されている。尚、実際に発行されたカードを認証するための認証装置としてのカードリーダ 3 は書き込み機能を除き、カードリーダライタ 2 と同様であるのでその詳細な説明を省略する。

【0018】以下に、図 4～図 6 に沿ってカード 4 の発行手順及び認証手順を説明する。証明装置 1 は、証明装置用秘密鍵データ 1A を用いて特定の署名生成ルールに

より各発行装置用公開鍵データ 2B を暗号化して証明装置署名データ 2C を生成するようになっている。この証明装置署名データ 2C は証明装置用公開鍵データ 1B を用いた特定の署名検査ルールによってのみ復号し得る。同様に、カードリーダーライタ 2 の制御ユニット 25 は、発行装置用秘密鍵データ 2A を用いた上記同様な署名生成ルールにより各カード 4 の後記する特徴データ 4D を暗号化して発行装置署名データ 4C を生成するようになっている。この発行装置署名データ 4C は発行装置用公開鍵データ 2B を用いた上記同様な署名検査ルールによってのみ復号し得る。

【0019】まず、図 4 に示すように、準備段階として、発行装置としてのカードリーダーライタ 2 に、発行装置用秘密鍵データ 2A、発行装置用公開鍵データ 2B、証明装置署名データ 2C 及び証明装置用公開鍵データ 1B を記憶しておく。このうち、発行装置用秘密鍵データ 2A、発行装置用公開鍵データ 2B、証明装置署名データ 2C は各発行機関固有のものである。

【0020】次に、図 5 に示すように、発行段階では、まず発行すべきカード 4 がカードリーダーライタ 2 に挿入されると、カードリーダーライタ 2 に設定された読み取り軌跡に沿って、基準領域 43 から物理的特徴を信号として機械的に読み取り、特徴データ 4D とする。この特徴データ 4D を発行装置用秘密鍵データ 2A を用いた署名生成ルールにより暗号化して発行装置署名データ 4C を生成する。そして、これら発行装置署名データ 4C、特徴データ 4D、発行装置用公開鍵データ 2B、証明装置署名データ 2C 及び証明装置用公開鍵データ 1B をカード 4 の磁気ストライプ 42 に格納する。

【0021】次に、図 6 に示すように、認証装置としてのカードリーダー 3 による認証段階では、まず認証すべきカード 4 がカードリーダー 3 に挿入されると、磁気ストライプ 42 に格納された発行装置署名データ 4C、特徴データ 4D、発行装置用公開鍵データ 2B、証明装置署名データ 2C 及び証明装置用公開鍵データ 1B を読み出すと共にカードリーダー 4 に設定された読み取り軌跡に沿って、基準領域 43 から物理的特徴を信号として機械的に読み取り、特徴データ 4D' とする。

【0022】そして、証明装置用公開鍵データ 1B を用いた署名検査ルールによって証明装置署名データ 2C を復号し、これを発行装置用公開鍵データ 2B と照合する。

【0023】同様に発行装置用公開鍵データ 2B を用いた署名検査ルールによって発行装置署名データ 4C を復号し、これを特徴データ 4D と照合する。

【0024】また、上記のように読み取った特徴データ 4D' と特徴データ 4D とを照合する。

【0025】上記各照合結果が所定の条件（各データ同士が一致、または不一致の程度が所定の範囲に収まっているなど）に一致したら、そのカード 4 が正規のカード

であると判定する。

【0026】図 7、図 8 は、本発明が適用された第 2 の実施形態に於ける認証式セキュリティシステムに於けるカードの発行手順及び認証手順を説明する図であり、第 1 の実施形態に於ける図 5、図 6 に対応する。このシステムも上記同様クレジットカードにおける認証式セキュリティシステムであり、その構成は第 1 の実施形態と同様である。

【0027】まず、準備段階としては上記同様にカードリーダーライタ 2 に、発行装置用秘密鍵データ 2A、発行装置用公開鍵データ 2B、証明装置署名データ 2C 及び証明装置用公開鍵データ 1B を記憶しておく。

【0028】次に、図 7 に示すように、発行段階では、まず発行すべきカード 4 がカードリーダーライタ 2 に挿入されると、カードリーダーライタ 2 に設定された読み取り軌跡に沿って、基準領域 43 から物理的特徴を信号として機械的に読み取り、そのデータ 4D を例えば 10 分割して特徴データ 4D1～4D10 とする。この特徴データ 4D1～4D10 を発行装置用秘密鍵データ 2A を用いた署名生成ルールにより暗号化して各々対応する発行装置署名データ 4C1～4C10 を生成する。そして、これら発行装置署名データ 4C1～4C10、これに対応する特徴データ 4D1～4D10、発行装置用公開鍵データ 2B、証明装置署名データ 2C 及び証明装置用公開鍵データ 1B をカード 4 の磁気ストライプ 42 に格納する。

【0029】次に、図 8 に示すように、カードリーダー 3 による認証段階では、まず認証すべきカード 4 がカードリーダー 3 に挿入されると、磁気ストライプ 42 に格納された発行装置用公開鍵データ 2B、証明装置署名データ 2C 及び証明装置用公開鍵データ 1B を読み出すと共に発行装置署名データ 4C1～4C10 及びこれに対応する特徴データ 4D1～4D10 の中から認証の度に異なる 1 つまたは複数の発行装置署名データと特徴データとの組を読み出す。更にカードリーダー 4 に設定された読み取り軌跡に沿って、基準領域 43 から物理的特徴を信号として機械的に読み取り、特徴データ 4D' とする。

【0030】そして、証明装置用公開鍵データ 1B を用いた署名検査ルールによって証明装置署名データ 2C を復号し、これを発行装置用公開鍵データ 2B と照合する。

【0031】同様に、例えば今回の認証で発行装置署名データ 4C5 及びこれに対応する特徴データ 4D5 を読み出したとして、発行装置用公開鍵データ 2B を用いた署名検査ルールによって発行装置署名データ 4C5 を復号し、これを特徴データ 4D5 と照合する。

【0032】また、特徴データ 4D5 と上記のように読み取った特徴データ 4D' の対応部分とを照合する。

【0033】上記各照合結果が所定の条件（各データ同士が一致、または不一致の程度が所定の範囲に収まって

いるなど)に一致したら、そのカード4が正規のカードであると判定する。

【0034】この構成によれば、カードリーダ3による読み出し内容が認証の度に異なることから、両者間のデータ授受を傍受してもその解析、またはカードに格納されたデータを偽造カードに利用することは困難になる。また、この処理は従来カード(被認証物)側で複雑な処理を行っていた動的認証方法と同程度のセキュリティ性を実現しながら、カード側にはデータ格納領域を確保すれば良く、その構造が簡便化されると共にコストが低廉になっている。

【0035】尚、上記構成では1つの特徴データを分割して複数の特徴データとしたが、基準領域43の読み取り位置をずらして複数回読み取っても良い。

【0036】図9、図10は、本発明が適用された第3の実施形態に於ける認証式セキュリティシステムに於けるカードの発行手順及び認証手順を説明する図であり、第1の実施形態に於ける図5、図6に対応する。このシステムも上記同様クレジットカードにおける認証式セキュリティシステムであり、その構成は第1の実施形態と概ね同様であるが、カード4には磁気ストライプに代えてデータ記憶及び演算処理が可能なIC45及び接点(図示せず)が設けられ、カードリーダライタ2及びカードリーダ3には磁気ヘッドに代えてIC45の接点に接触するための対応接点(図示せず)が設けられている。カードリーダ3は、(疑似)乱数からなる確認データRを生成するようになっている。また、IC45は、被認証物用秘密鍵データ4Aを用いて上記各実施形態と同様な署名生成ルールによりカードリーダ3側から送られる乱数からなる確認データRを暗号化して被認証物署名データ4Cを生成するようになっている。

【0037】まず、準備段階としては上記同様にカードリーダライタ2に、発行装置用秘密鍵データ2A、発行装置用公開鍵データ2B、証明装置署名データ2C、証明装置用公開鍵データ1B、各カード4毎に設定される被認証者用秘密鍵データ4A及び被認証者用公開鍵データ4Bを用意しておく。

【0038】次に、図9に示すように、発行段階では、まず発行すべきカード4がカードリーダライタ2に挿入されると、カードリーダライタ2に設定された読み取り軌跡に沿って、基準領域43から物理的特徴を信号として機械的に読み取り、特徴データ4Dとする。この特徴データ4Dを発行装置用秘密鍵データ2Aを用いた署名生成ルールにより暗号化して発行装置署名データ4Cを生成する。そして、これら発行装置署名データ4C、特徴データ4D、発行装置用公開鍵データ2B、証明装置署名データ2C、証明装置用公開鍵データ1B、認証者用秘密鍵データ4A及び被認証者用公開鍵データ4Bをカード4のIC45の記憶領域に格納する。

【0039】次に、図10に示すように、カードリーダ

3による認証段階では、まず認証すべきカード4がカードリーダ3に挿入されると、IC45の記憶領域に格納された発行装置署名データ4C、特徴データ4D、発行装置用公開鍵データ2B、証明装置署名データ2C、証明装置用公開鍵データ1B及び被認証者用公開鍵データ4Bを読み出すと共にカードリーダ3に設定された読み取り軌跡に沿って、基準領域43から物理的特徴を信号として機械的に読み取り、特徴データ4D'とする。また、カードリーダ3側にて乱数を発生させ、これを確認データRとしてIC45に送る。

【0040】このとき、特徴データ4D'は疑似乱数でなく自然の乱数であることから、この一部やこれを何らかのアルゴリズムで処理したもの、或いは特徴データ4D'を抽出するのと同様な方法を用いて基準領域の一部や基準領域以外の領域から抽出したデータを確認データRとして利用しても良い。これにより、疑似乱数の解析による乱数が特定されることを防止でき、セキュリティ性が一層向上する。所謂Fault-based attack等のように、CPUに対して外部から様々な刺激を与えることにより誤動作を起こさせるような攻撃方法も人為的な操作が介在する余地が殆どない方法によって発生した物理的な特徴を乱数として使用することにより防止できる。

【0041】そして、証明装置用公開鍵データ1Bを用いた署名検査ルールによって証明装置署名データ2Cを復号し、これを発行装置用公開鍵データ2Bと照合する。

【0042】同様に、発行装置用公開鍵データ2Bを用いた署名検査ルールによって発行装置署名データ4Cを復号し、これを特徴データ4Dと照合する。

【0043】また、IC45では確認データRを被認証物用秘密鍵データ4Aを用いた署名生成ルールにより暗号化して被認証物署名データ4Eを生成し、これをカードリーダ3側に送り返す。カードリーダ3では被認証物用公開鍵データ4Bを用いた署名検査ルールによって被認証物署名データ4Eを復号し、これを確認データRと照合する。

【0044】更に、特徴データ4Dと上記のように読み取った特徴データ4D'とを照合する。

【0045】上記各照合結果が所定の条件(各データ同士が一致、または不一致の程度が所定の範囲に収まっているなど)に一致したら、そのカード4が正規のカードであると判定する。

【0046】この構成によれば、上記同様カードリーダ3による読み出し内容が認証の度に異なることから、両者間のデータ授受を傍受してもその解析、またはカードに格納されたデータを偽造カードに利用することは困難になる。

【0047】尚、上記各実施形態では被認証物に証明装置用公開鍵データ1Bを記憶させ、署名検査ルールによ

って証明装置署名データ2Cを復号し、これを発行装置用公開鍵データ2Bと照合したが、この処理は任意であり、例えば証明機関と発行機関が同じ場合には省略することができる。また、証明機関が1つであり、その証明機関用秘密鍵データ1A、証明機関用公開鍵データ1Bの変更がない場合、証明機関用公開鍵データ1Bは必ずしも被認証物側に記憶させておく必要はなく、認証装置製造時にこの認証装置に記憶させておいても良い。このようにすれば、独自に各秘密鍵データ、公開鍵データをも偽造しても証明機関用公開鍵データ1Bのみは正規なものを使わざるを得ないことから証明機関の秘密鍵データを知られない限り、上記照合が一致せず、チェックできることから、証明機関用秘密鍵データ及び公開鍵データの変更がないシステムの場合、そのメンテナンス性が低下することなくセキュリティ性が向上する。

【0048】また、認証装置を、必要なときに証明装置と接続可能とし、かつ過去の認証時に被認証物から読み出された証明装置用公開鍵データを1つまたは2つ以上記憶可能とし、認証時に被認証物から読み出された証明装置用公開鍵データを記憶された証明装置用公開鍵データと比較し、一致すれば該証明装置用公開鍵データを用いて上記照合を行い、一致しなければ証明装置に通信等で問い合わせて正規の証明装置用公開鍵データであることが確認されたら該証明装置用公開鍵データを用いて照合を行うようにし、確認された該証明装置用公開鍵データを追加して記憶、または問い合わせ結果によっては変更するようにしても良い。この場合も独自に各秘密鍵データ、公開鍵データをも偽造しても証明機関用公開鍵データ1Bのみは正規なものを使わざるを得ないことから証明機関の秘密鍵データを知られない限り、上記照合が一致せず、チェックできる。従ってそのメンテナンス性が低下することなくセキュリティ性が向上する。更にこの構造では証明機関用秘密鍵データ及び公開鍵データが変更されても認証装置全てを同時に更新する必要はなく、認証時に新しい証明機関用公開鍵データが被認証物から読み出された場合にのみこれを追加して記憶、または新しいデータに置き換えれば良いことから証明装置用公開鍵データを認証装置にのみ記憶するシステムに比較してそのメンテナンス性が高くなっている。この認証装置のメンテナンス構造は、常にサーバと接続され、IDや暗証番号、認証コードなどを確認するような端末機を有するシステムに一般的に単独で応用でき、サーバや接続回線の負荷が低減できるものである。

【0049】また、上記各実施形態では被認証物をクレジットカードとしたが、例えばプリペイドカードやIDカード、固有の価値が証明された貴金属類、有価証券、部屋や自動車のキーなど、真正なものであることを証明する必要のあるものに任意に適用できることは言うまでもない。また、第1及び第2の実施形態では被認証物のデータ格納領域を磁気ストライプとしたが、第3の実

形態のようにICチップをカードに埋め込んでICカードとしても良い。

【0050】

【発明の効果】このように、本発明によれば、人為的に同一なものを製作することが困難な基準領域の特徴データ、この特徴データを発行装置用秘密鍵データにより暗号化して生成された署名データ及び発行装置用公開鍵データを被認証物のデータ格納領域に格納しておき、これを認証時に読み出すと共にその基準領域の特徴を読み取り、これらの照合結果により被認証物の真正性を確認できるようにしたため、秘密鍵データを知らずに署名データを解析することは著しく困難であり、また被認証物のデータ格納領域に格納されたデータを単にデッドコピーしても他の被認証物では基準領域の特徴が異なることからその真正性は否定されるため他の被認証物への不正な適用をも効果的に防止することができ、しかも認証に必要なデータが全て被認証物側にあることから、認証装置側の記憶容量を著しく低減でき、また発行装置用秘密鍵データや発行装置用公開鍵データを変更したり新たな発行装置用秘密鍵データや発行装置用公開鍵データを追加しても認証装置側の更新を必要としないことからその保守が極めて簡便になる。

【0051】特に、認証の度に被認証物と認証装置との通信内容を変えるようにする場合、請求項2のように被認証物側に格納された複数のデータの1つまたは幾つかを認証装置側で選択して読み出すようにすることで、被認証物側に演算処理のためのIC等を設ける必要がなく、しかも処理が簡便になる。

【図面の簡単な説明】

【図1】本発明に基づくシステムの概略構成を示すブロック図。

【図2】本発明に基づくシステムが適用された記録媒体の一例としてのプリペイドカードを示す正面図。

【図3】プリペイドカードのためのカードリーダーの一例を示すダイアグラム図。

【図4】本発明に基づく第1の実施形態に於けるカードの作成手順を示すブロック図。

【図5】本発明に基づく第1の実施形態に於けるカードの作成手順を示すブロック図。

【図6】本発明に基づく第1の実施形態に於けるカードの認証手順を示すブロック図。

【図7】本発明に基づく第1の実施形態に於けるカードの作成手順を示すブロック図。

【図8】本発明に基づく第1の実施形態に於けるカードの認証手順を示すブロック図。

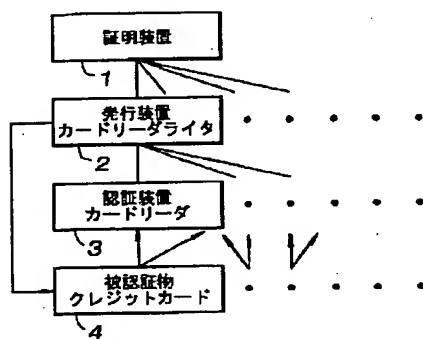
【図9】本発明に基づく第1の実施形態に於けるカードの作成手順を示すブロック図。

【図10】本発明に基づく第1の実施形態に於けるカードの認証手順を示すブロック図。

【符号の説明】

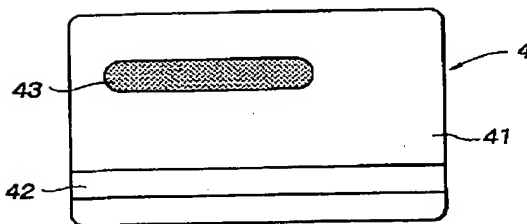
- 1 証明装置
- 2 カードリーダーライター (発行装置)
- 21 スロット
- 22 カード搬送ユニット
- 23 磁気ヘッド
- 24 誘導式磁気ヘッド
- 25 制御ユニット
- 3 カードリーダー (認証装置)
- 4 クレジットカード (被認証物)
- 41 ベースシート
- 42 磁気ストライプ
- 43 基準領域
- 45 IC
- 1A 証明装置用秘密鍵データ

【図 1】

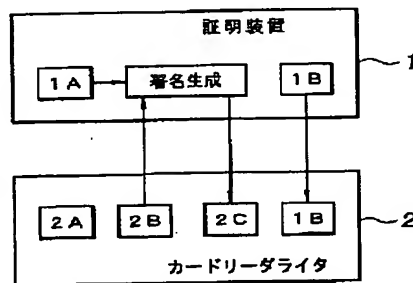


- 1B 証明装置用公開鍵データ
- 2A 発行装置用秘密鍵データ
- 2B 発行装置用公開鍵データ
- 2C 証明装置署名データ
- 4A 被認証物用秘密鍵データ
- 4B 被認証物用公開鍵データ
- 4C 発行装置署名データ
- 4C1~4C10 特徴データ 4D1~4D10に対応する発行装置署名データ
- 4D 特徴データ
- 4D' 認証時に読み取った特徴データ
- 4D1~4D10 特徴データ 4Dの分割データ
- 4E 被認証物署名データ
- R 確認データ (乱数)

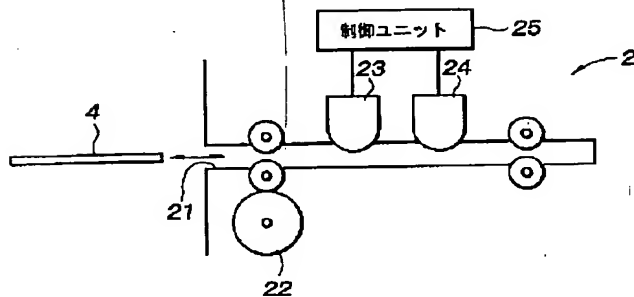
【図 2】



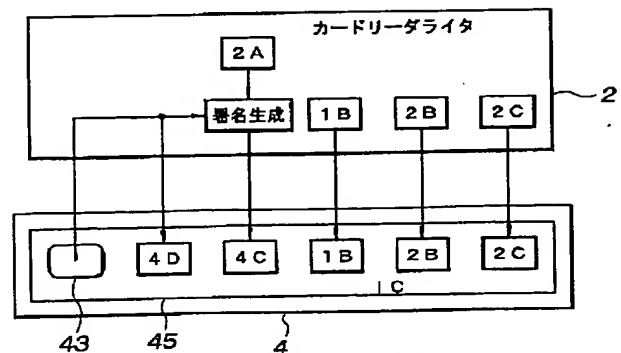
【図 4】



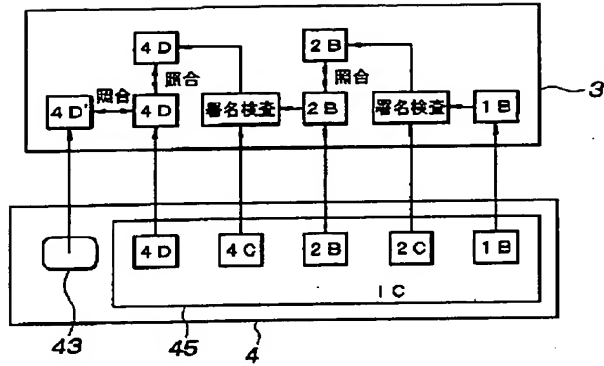
【図 3】



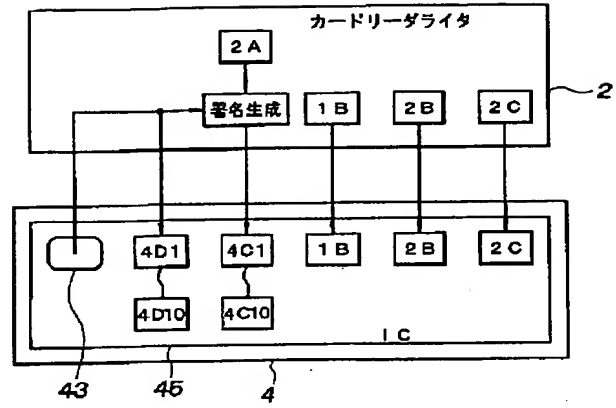
【図 5】



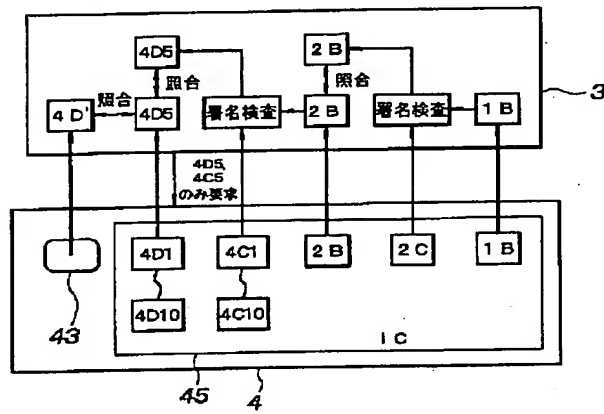
【図 6】



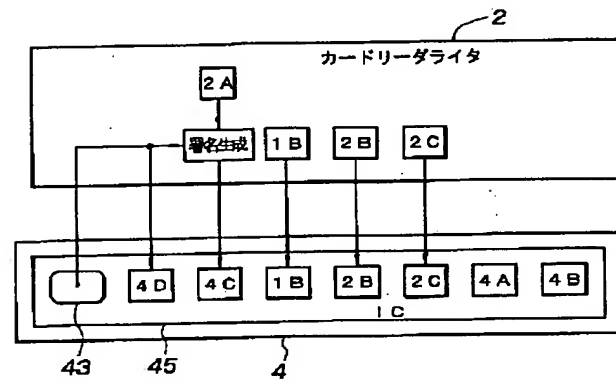
【図 7】



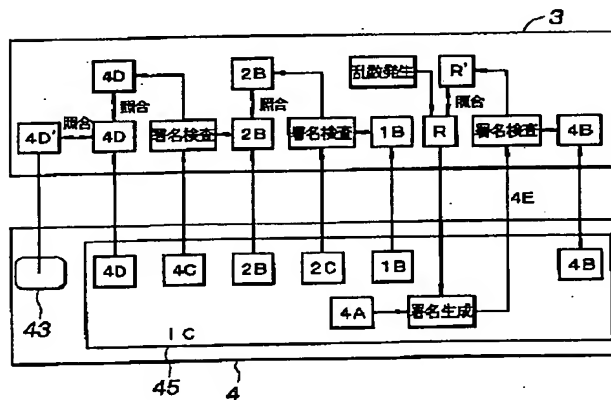
【図 8】



【図 9】



【図 10】



フロントページの続き

(72)発明者 山本屋 健二
神奈川県横浜市金沢区福浦 3 丁目 10 番地
日本発条株式会社内